Chapter 14
Security and Privacy Concerns of Virtual Worlds

Greg Gogolin
Ferris State University, USA

ABSTRACT
This chapter looks at security and privacy concerns of virtual worlds by investigating the use and capabilities of current and emerging technologies such as gaming, blogging, podcasting, virtual meetings, and virtual worlds. Security and privacy concerns will be investigated in the context of exploits and IT-related security risks, access management and confidentiality, reputation and product risk management, resource management, financial considerations and accountability, and safety. Several technologies and personal practices are reviewed, as well as ways to mitigate or eliminate their associated risks. The core principles of information security - confidentiality, integrity, and availability - provide an overall framework for the chapter.

INTRODUCTION
Digitally created worlds are changing the face of E-Commerce and extending the use of Internet technologies to create a more immersive experience for customers. With the challenges in things such as identity theft, fraud and virtual stalking, businesses will not be able to fully leverage Virtual Worlds if they fail to address security and privacy concerns.

This chapter will investigate the use and capabilities of current and emerging technologies such as gaming, blogs, podcasting, virtual meetings and virtual worlds in the context of their productive utility and security risks presented. Security and privacy concerns will be investigated in the following areas:

1. Exploits and IT-Related Security Risks
2. Access Management and Confidentiality
3. Reputation and Product Risk Management
4. Resource Management

DOI: 10.4018/978-1-61692-808-7.ch014
5. Financial Considerations and Accountability
6. Safety

The chapter will conclude with a summary and a look at emerging trends and future direction in security and privacy of virtual worlds and E-Commerce.

BACKGROUND

In the late 1990’s, E-Commerce was hyped as a way for small start-up companies to compete on a level playing field with established corporate behemoths. The demise of brick and mortar stores was widely predicted and common sense business practices were thought of as outdated. The “Internet Bubble” burst by 2001 and most realized the error in forgetting the basics. Companies learned a lot about the Internet, E-Commerce and their business during the Bubble, but an area that lagged the Bubble in terms of attention and focus was that of security. Ten years later, hacking, identity theft, privacy and similar information security issues have become central to the business model.

Social networking through the use of Internet sites such as Facebook, MySpace, Twitter and LinkedIn became among the most popular uses of the Internet as the first decade of the new millennium drew to a close, with Facebook #2, MySpace #12, Twitter #14 and LinkedIn #39 in Alexa’s rankings of the top 500 global Internet sites (Alexa.com, 2009). Online gaming and virtual world technology have become mainstream, aided by the advancement of home gaming systems gaining Internet technology. This has led to massively multiplayer online role-playing games (MMORPG), which can entail literally tens of thousands of players participating in an online gaming experience in a virtual world.

Virtual worlds like Second Life®, There.com, and more business-focused offerings are on the brink of becoming valuable work tools. Major companies and public-sector organizations such as BP, IBM, Intel, and the US Army are investing heavily in virtual world technologies. (Driver & Jackson, 2008). In fact, Driver and Jackson predict that by 2013 the 3-D Internet will be as important for work as the Web is today. This view was supported in an article in CIO magazine (Lynch, 2008) that projected enterprise versions of online virtual worlds like Second Life® would be just as important to business as the Web is today. This may be a stretch because the same research organization (Forrester Research) recently reported that “only 11% of enterprises have adopted virtual worlds to augment their work.” (Rutherford, 2009).

From the point of view of most business leaders, the utility of virtual worlds in business is not apparent. Keitt (2009) attributes this to virtual world vendors not doing a particularly good job articulating their value. Instead, the central message of virtual world providers is that they allow for groupings that can be augmented or reduced on the fly while also allowing users to consider information from multiple applications simultaneously. King (2008) reports that companies such as IBM, Sun, Xerox, Cisco and Unilever are using 3D technology and virtual worlds in this very manner for things like strategy sessions, employee meetings, mixers, and recruiting. While the use of virtual worlds for functions such as E-commerce shows much promise, security and privacy are critical success factors. The purpose of this chapter is to investigate many of the issues that are part of the security and privacy equation for success.

ISSUES, CONTROVERSIES, PROBLEMS

The security and privacy concerns associated with virtual worlds and E-commerce are immense and multi-faceted. This is an environment where people and organizations are asked to trust that which may not be real or easily verified. Because this is a rapidly evolving situation and set of circumstances that in many cases break precedent, the societal norms, laws, ethics and values struggle to adapt.